PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-304227
(43)Date of publication of application : 24.10.2003

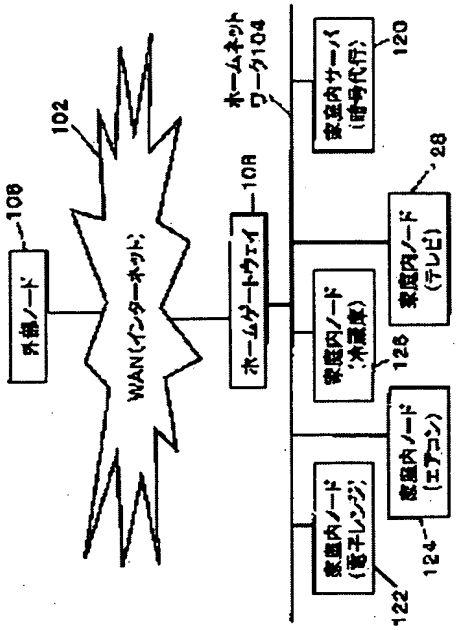
(51)Int.CI. H04L 9/08
H04L 12/66

(21)Application number : 2002-104846
(22)Date of filing : 08.04.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NODA TAKESHI

(54) CRYPTOGRAPHIC COMMUNICATION APPARATUS, ITS METHOD AND CRYPTOGRAPHIC COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To allow even equipment such as a home electric product having no advanced information processing capacity to perform advanced cryptographic communication through an external open type network and to highly keep the security of the cryptographic communication.
SOLUTION: A cryptographic communication apparatus is provided with a first network, first terminal equipment connected to the first network, a cryptographic communication deputizing server connected to the first network, a second network connected to the first network through a gateway, and second terminal equipment connected to the second network. In performing cryptographic communication between the first terminal equipment and the second terminal equipment, the cryptographic communication deputizing server performs encryption and decryption instead of the first terminal equipment.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

特1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－304227
（P2003－304227A）
(43)公開日　平成15年10月24日(2003.10.24)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　12/66	Ｂ　５Ｊ１０４
12/66		9/00	６０１Ｚ　５Ｋ０３０

審査請求　未請求　請求項の数30　ＯＬ　（全 13 頁）

(21)出願番号　特願2002－104846(P2002－104846)

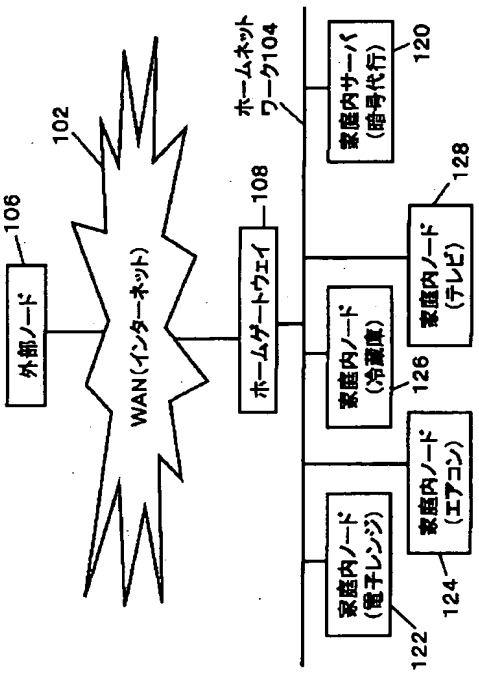
(22)出願日　平成14年４月８日(2002.4.8)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　野田　健
愛知県名古屋市中区栄２丁目６番１号白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

Ｆターム(参考)　5J104 AA17 NA43 PA07
5K030 GA15 HA08 HC13 JA07

(54)【発明の名称】　暗号通信装置、暗号通信方法及び暗号通信システム

(57)【要約】
【課題】　家庭内電気製品等の高度な情報処理能力を有さない機器であっても、外部の開放型ネットワークを経由し、高度な暗号通信を行うことを可能とし、そのセキュリティを高度に確保する。
【解決手段】　第１のネットワークと、前記第１のネットワークに接続された第１の端末装置と、前記第１のネットワークに接続された暗号通信代行サーバと、前記第１のネットワークとゲートウェイを介して接続された第２のネットワークと、前記第２のネットワークに接続された第２の端末装置とを有し、前記第１の端末装置と前記第２の端末装置が暗号通信を行う時、前記第１の端末装置に代わって前記暗号通信代行サーバが暗号化と復号化を行う。



1

【特許請求の範囲】

【請求項１】　第１のネットワークと、

前記第１のネットワークに接続された第１の端末装置と、

前記第１のネットワークに接続された暗号通信代行サーバと、

前記第１のネットワークとゲートウェイを介して接続された第２のネットワークと、

前記第２のネットワークに接続された第２の端末装置とを有し、

前記第１の端末装置と前記第２の端末装置が暗号通信を行う時、前記第１の端末装置に代わって前記暗号通信代行サーバが暗号化と復号化を行う、暗号通信システム。

【請求項２】　前記第１のネットワークはアクセスが制限された閉鎖型ネットワークであり、

前記第２のネットワークはアクセスが自由な開放型ネットワークである、請求項１に記載の暗号通信システム。

【請求項３】　前記第２の端末装置は、暗号通信要求データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記第１の端末装置へ送り、

前記第１の端末装置は、暗号通信承諾データと暗号通信代行サーバ指定データを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して、前記第２の端末装置へ送り、

前記第２の端末装置は、暗号化データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記暗号通信代行サーバへ送る、請求項１又は請求項２に記載の暗号通信システム。

【請求項４】　前記第２の端末装置は、非暗号化データ又は前記第１の端末装置が復号化できない暗号化データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記第１の端末装置へ送り、

前記第１の端末装置は、暗号通信依頼データと暗号通信代行サーバ指定データを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して、前記第２の端末装置へ送り、

前記第２の端末装置は、暗号化データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記暗号通信代行サーバへ送る、請求項１から請求項３の何れか１項に記載の暗号通信システム。

【請求項５】　前記第２の端末装置は、更に暗号通信代行要求データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記暗号通信代行サーバへ送り、

前記暗号通信サーバは、暗号通信代行承諾データを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して、前記第２の端末装置へ送

2

る、請求項３又は請求項４に記載の暗号通信システム。

【請求項６】　前記第１の端末装置は、暗号通信代行要求データを、前記第１のネットワークを経由して、前記暗号通信代行サーバへ送り、

前記暗号通信代行サーバは、暗号通信要求データを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して、前記第２の端末装置へ送り、

前記第２の端末装置は、暗号通信承諾データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記暗号通信代行サーバへ送り、

前記暗号通信承諾データを受信した暗号通信代行サーバは、前記第１の端末装置へ、暗号通信代行承諾データを、前記第１のネットワークを経由して送り、

前記暗号通信代行承諾データを受信した前記第１の端末装置は、非暗号化データを、前記第１のネットワークを経由して、前記暗号通信代行サーバへ送り、

前記非暗号化データを受信した暗号通信代行サーバは、前記第２の端末装置へ、前記非暗号化データを暗号化したデータを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して送信する、請求項１から請求項５の何れか１項に記載の暗号通信システム。

【請求項７】　アクセスが制限された閉鎖型ネットワークに接続され、

前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して行わせる、暗号通信装置。

【請求項８】　前記開放型ネットワークに接続された端末装置から、前記開放型ネットワークとゲートウェイと閉鎖型ネットワークとを経由して暗号通信要求データを受信し、

前記端末装置に暗号通信承諾データと前記閉鎖型ネットワークに接続された暗号通信代行サーバの指定とを、前記閉鎖型ネットワークとゲートウェイと開放型ネットワークとを経由して送信する、請求項７に記載の暗号通信装置。

【請求項９】　前記開放型ネットワークに接続された端末装置から、前記開放型ネットワークとゲートウェイと閉鎖型ネットワークとを経由して非暗号化データ又は復号化できない暗号化データを受信し、

前記端末装置に暗号通信承諾データと前記閉鎖型ネットワークに接続された暗号通信代行サーバの指定とを、前記閉鎖型ネットワークとゲートウェイと開放型ネットワークとを経由して送信する、請求項７又は請求項８に記載の暗号通信装置。

【請求項１０】　前記開放型ネットワークに接続された端末装置に暗号化データを送信するための暗号通信代行

要求データを、前記閉鎖型ネットワークに接続された暗号通信代行サーバに、前記閉鎖型ネットワークを経由して送信する、請求項７から請求項９の何れか１項に記載の暗号通信装置。

【請求項１１】　前記暗号通信代行サーバからの暗号通信代行承諾データを、前記閉鎖型ネットワークを経由して受信し、

前記暗号通信代行サーバへ、前記開放型ネットワークに接続された端末装置に暗号化して送信するためのデータを非暗号化の状態で、前記閉鎖型ネットワークを経由して送信する、請求項７から請求項１０の何れか１項に記載の暗号通信装置。

【請求項１２】　アクセスが制限された閉鎖型ネットワークに接続され、

前記閉鎖型ネットワークに接続された第１の端末装置と、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された第２の端末装置との間の暗号通信を、

前記第１の端末装置に代行して行う、暗号通信代行サーバ。

【請求項１３】　前記開放型ネットワークに接続された第２の端末装置から、前記開放型ネットワークとゲートウェイと閉鎖型ネットワークとを経由して暗号化データを受信し、

前記暗号化データを復号し、

前記復号化データを前記閉鎖型ネットワークに接続された第１の端末装置へ、前記閉鎖型ネットワークを経由して送信する、請求項１２に記載の暗号通信代行サーバ。

【請求項１４】　前記開放型ネットワークに接続された第２の端末装置から、前記開放型ネットワークとゲートウェイと閉鎖型ネットワークとを経由して、暗号通信代行要求データを更に受信し、

前記第２の端末装置に、閉鎖型ネットワークとゲートウェイと開放型ネットワークとを経由して暗号通信代行承諾データを送信する、請求項１３に記載の暗号通信代行サーバ。

【請求項１５】　前記閉鎖型ネットワークに接続された第１の端末装置から、前記閉鎖型ネットワークを経由して、非暗号化データを受信し、

前記非暗号化データを暗号化し、

前記暗号化データを、開放型ネットワークに接続された第２の端末装置に、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して送信する、請求項１２から請求項１４の何れか１項に記載の暗号通信代行サーバ。

【請求項１６】　前記開放型ネットワークに接続された前記第２の端末装置に、暗号通信要求データを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して更に送信し、

前記開放型ネットワークに接続された前記第２の端末装置から、暗号通信承諾データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して受信し、

前記閉鎖型ネットワークに接続された第１の端末装置に、暗号通信代行承諾データを、前記閉鎖型ネットワークを経由して送信する、請求項１５に記載の暗号通信代行サーバ。

【請求項１７】　アクセスが自由な開放型ネットワークに接続され、

前記開放型ネットワークとゲートウェイを経由して接続された閉鎖型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行させる、暗号通信装置。

【請求項１８】　前記閉鎖型ネットワークに接続された端末装置に、暗号通信要求データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信し、

前記閉鎖型ネットワークに接続された端末装置から、暗号通信承諾データと前記閉鎖型ネットワークに接続された暗号通信代行サーバの指定データとを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信し、

前記暗号通信代行サーバに、暗号化データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信する、請求項１７に記載の暗号通信装置。

【請求項１９】　前記閉鎖型ネットワークに接続された端末装置に、非暗号化データ又は前記端末装置が復号化できない暗号化データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信し、

前記閉鎖型ネットワークに接続された端末装置から、暗号通信依頼データと前記閉鎖型ネットワークに接続された暗号通信代行サーバの指定データとを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信し、

前記暗号通信代行サーバに、暗号化データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信する、請求項１７又は請求項１８に記載の暗号通信装置。

【請求項２０】　前記閉鎖型ネットワークに接続された暗号通信代行サーバに、暗号通信代行要求データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して更に送信し、

前記閉鎖型ネットワークに接続された暗号通信代行サーバから、暗号通信代行承諾データを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信する、請求項１８又は請求項１９に記載の暗号通信装置。

【請求項２１】　閉鎖型ネットワークに接続された暗号

通信代行サーバから、暗号通信要求データを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信し、
前記閉鎖型ネットワークに接続された暗号通信代行サーバに、暗号通信承諾データを、前記開放型閉鎖型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信し、
前記閉鎖型ネットワークに接続された暗号通信代行サーバから、暗号化データを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信する、請求項１７から請求項２０の何れか１項に記載の暗号通信装置。
【請求項２２】　第１のネットワークと、
前記第１のネットワークに接続された第１の端末装置と、
前記第１のネットワークに接続された暗号通信代行サーバと、
前記第１のネットワークとゲートウェイを介して接続された第２のネットワークと、
前記第２のネットワークに接続された第２の端末装置と、を使用する暗号通信方法で、
前記第１の端末装置と前記第２の端末装置が暗号通信を行う時、前記第１の端末装置に代わって前記暗号通信代行サーバが暗号化と復号化を実行する、暗号通信方法。
【請求項２３】　アクセスが制限された閉鎖型ネットワークに接続された暗号通信装置が実行する暗号通信方法で、
前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して実行させる、暗号通信方法。
【請求項２４】　アクセスが制限された閉鎖型ネットワークに接続された暗号通信代行サーバが実行する暗号通信方法で、
前記閉鎖型ネットワークに接続された第１の端末装置と、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された第２の端末装置との間の暗号通信を、前記第１の端末装置に代行して実行する、暗号通信方法。
【請求項２５】　アクセスが自由な開放型ネットワークに接続された暗号通信装置が実行する暗号通信方法で、
前記開放型ネットワークとゲートウェイを経由して接続された閉鎖型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して実行させる、暗号通信方法。
【請求項２６】　第１のネットワークと、
前記第１のネットワークに接続された第１の端末装置と、
前記第１のネットワークに接続された暗号通信代行サーバと、

前記第１のネットワークとゲートウェイを介して接続された第２のネットワークと、
前記第２のネットワークに接続された第２の端末装置と、で実行されるコンピュータプログラムで、
前記第１の端末装置と前記第２の端末装置が暗号通信を行う時、前記第１の端末装置に代わって前記暗号通信代行サーバが暗号化と復号化を実行するための、暗号通信コンピュータプログラム。
【請求項２７】　アクセスが制限された閉鎖型ネットワークに接続された暗号通信装置で実行されるコンピュータプログラムで、
前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して実行させるための、暗号通信コンピュータプログラム。
【請求項２８】　アクセスが制限された閉鎖型ネットワークに接続された暗号通信代行サーバで実行されるコンピュータプログラムで、
前記閉鎖型ネットワークに接続された第１の端末装置と、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された第２の端末装置との間の暗号通信を、前記第１の端末装置に代行して実行するための、暗号通信コンピュータプログラム。
【請求項２９】　アクセスが自由な開放型ネットワークに接続された暗号通信装置で実行されるコンピュータプログラムで、
前記開放型ネットワークとゲートウェイを経由して接続された閉鎖型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して実行させるための、暗号通信コンピュータプログラム。
【請求項３０】　請求項２６から請求項２９の何れか１項に記載したコンピュータプログラムを記録した、コンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークに接続された機器間で暗号化されたデータ通信（暗号通信）を行う装置、方法、コンピュータプログラム、コンピュータプログラムを記録した媒体に関するものである。
【０００２】特に、この暗号通信を行う機器が、家庭電気製品等、高度な情報処理性能を有しておらず、暗号化通信のためのデータ暗号化とデータ復号化のための処理を適切に行うことが出来ないため、これら本来自分が行うべきデータ暗号化とデータ復号化処理を、同じネットワークに接続された暗号通信代行サーバに行わせる暗号通信装置、暗号通信方法、暗号通信プログラム、暗号通信プログラムを記録した媒体に関するものである。
【０００３】

【従来の技術】従来の、データ暗号化とデータ復号化の処理を代行して行う暗号通信システムには、例えば、特開２００１-２３７８１８号公報に記載のものがあった。本暗号通信システムは、第１及び第２の通信装置の間の通信を中継する機能を具備した第３の通信装置（プロキシサーバ）が、前記第１及び第２の通信装置のうち一方の通信装置と前記第３の通信装置（プロキシサーバ）との間の通信に用いられる暗号鍵を前記第１及び第２の通信装置の他方の通信装置に通知する手段を備え、前記他方の通信装置では前記通知された暗号鍵を用いて前記第３の通信装置（プロキシサーバ）との間の通信を行い、前記第１及び第２の通信装置間の前記第３の通信装置（プロキシサーバ）を中継した暗号通信を同一の暗号鍵を用いて行うことで、前記第３の通信装置（プロキシサーバ）における暗号化及び復号化処理を省略するようにしたことを特徴とする。

【０００４】本従来の暗号通信システムの一実施の形態を図５に示す。例えば、図５に示す外部端末装置９０６が第１及び第２の通信装置のうち一方の通信装置に該当し、内部端末装置９２２が第１及び第２の通信装置のうち他方の通信装置に該当し、中継装置９０８が第３の通信装置（プロキシサーバ）に該当する。

【０００５】中継装置９０８は、外部端末装置９０６との通信に用いる暗号鍵を内部端末装置９２２に通知する（Ｓ９１）。その後、外部端末装置９０６と内部端末装置９２２との間の通信は、その鍵を使った暗号化データで行われるが、中継装置９０８は、データの中継は行うが、その鍵を使って暗号化と復号化の処理は行わない（Ｓ９２）。暗号化と復号化の処理は、外部端末装置９０６と、内部端末装置９２２によって行われる（Ｓ９３）。

【０００６】

【発明が解決しようとする課題】しかしながら、前記従来の暗号通信システムでは、確かに前記第３の通信装置（第１の通信装置と第２の通信装置の間の通信を中継するプロキシサーバ）の負荷は軽減されるが、その一方、第１の通信装置又は第２の通信装置の負荷は逆に増大する。確かに、前記第３の通信装置（第１の通信装置と第２の通信装置の間の通信を中継するプロキシサーバ）の負荷が軽減されることは、本通信装置が多くの端末装置間の通信を中継し、その負荷が余りに大きいケースでは利益があることも考えられる。

【０００７】更に、通信を行う第１の端末装置と第２の端末装置のデータ処理性能が充分大きい時（例えば、パーソナルコンピュータ等のデータ処理装置である時）には、不利益は無いかも知れない。しかしながら、現在のように社会の情報化とデータ通信ネットワークが普及した時代では、ネットワークに接続される機器は、必ずしもデータ処理性能が充分大きい、例えば、パーソナルコンピュータ等のデータ処理装置とは限らない。例えば、現在、パーソナルコンピュータは勿論、様々な携帯情報端末、携帯電話、更には、カーナビ、セットトップボックス等がデータ通信ネットワークに接続されている。

【０００８】更に今後は、その他多くの家庭内電気製品、例えば、テレビ、ビデオレコーダー、ビデオカメラ、オーディオ機器、ラジオ、冷蔵庫、電子レンジ、オーブン、洗濯機、乾燥機、掃除機、エアコン、照明器具、その他家庭内に存在するあらゆる電気製品がデータ通信ネットワークに接続される。特に、データ通信のためのプロトコルとしてＩＰｖ６が普及すれば、インターネットアドレスの不足問題が一気に解消され、これらのことが益々現実のものとなる。

【０００９】しかし又、このように家庭内電気製品が家庭外のネットワークに接続されるようになると、家庭内電気製品を家庭の外から自由にモニタし、コントロール可能となって、便利となる反面、セキュリティの大きな問題が発生する可能性がある。例えば、悪意を持つ者に、家庭内の種々の家庭内電気製品が不法にモニタされ、コントロールされる可能性が生じる。

【００１０】このような時には、これら家庭内電気製品のデータ通信におけるセキュリティ確保が大きな意義を持つこととなり、そのための一つの解決策がデータを暗号化した通信である。しかし又、高度なデータ暗号化と復号化を行うには、それを行う機器に大きなデータ処理性能が必要になる。充分なセキュリティレベルを確保するには、当然それに見合う高度な暗号化と復号化を行わなければならない。更に又、このような全ての家庭内電化製品が、これら高度の暗号化と復号化を行うのに必要なデータ処理性能を有しているとは限らず、むしろ逆に、このようなデータ処理性能を有していないことが多いと思われる。

【００１１】これら家庭内電気製品が本来の役割を果たすだけのためには、それほど大きなデータ処理性能は必要でなく、各家庭内電気製品が家庭外のネットワークと接続され、データ通信のセキュリティを確保するだけのために、全ての家庭内電気製品が、高度なデータ暗号化と復号化を実行するためのデータ処理性能を持つことは無駄が多い。

【００１２】

【課題を解決するための手段】上記課題を解決するため、本発明の第１の暗号通信システムでは、第１のネットワークと、前記第１のネットワークに接続された第１の端末装置と、前記第１のネットワークに接続された暗号通信代行サーバと、前記第１のネットワークとゲートウェイを介して接続された第２のネットワークと、前記第２のネットワークに接続された第２の端末装置とを有し、前記第１の端末装置と前記第２の端末装置が暗号通信を行う時、前記第１の端末装置に代わって前記暗号通信代行サーバが暗号化と復号化を行う。

【００１３】本発明の第２の暗号通信システムでは、前

記第１のネットワークはアクセスが制限された閉鎖型ネットワークであり、前記第２のネットワークはアクセスが自由な開放型ネットワークである。

【００１４】本発明の第３の暗号通信システムでは、前記第２の端末装置は、暗号通信要求データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記第１の端末装置へ送り、前記第１の端末装置は、暗号通信承諾データと暗号通信代行サーバ指定データを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して、前記第２の端末装置へ送り、前記第２の端末装置は、暗号化データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記暗号通信代行サーバへ送る。

【００１５】本発明の第４の暗号通信システムでは、前記第２の端末装置は、非暗号化データ又は前記第１の端末装置が復号化できない暗号化データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記第１の端末装置へ送り、前記第１の端末装置は、暗号通信依頼データと暗号通信代行サーバ指定データを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して、前記第２の端末装置へ送り、前記第２の端末装置は、暗号化データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記暗号通信代行サーバへ送る。

【００１６】本発明の第５の暗号通信システムでは、前記第２の端末装置は、更に暗号通信代行要求データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記暗号通信代行サーバへ送り、前記暗号通信サーバは、暗号通信代行承諾データを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して、前記第２の端末装置へ送る。

【００１７】本発明の第６の暗号通信システムでは、前記第１の端末装置は、暗号通信代行要求データを、前記第１のネットワークを経由して、前記暗号通信代行サーバへ送り、前記暗号通信代行サーバは、暗号通信要求データを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して、前記第２の端末装置へ送り、前記第２の端末装置は、暗号通信承諾データを、前記第２のネットワークと前記ゲートウェイと前記第１のネットワークとを経由して、前記暗号通信代行サーバへ送り、前記暗号通信承諾データを受信した暗号通信代行サーバは、前記第１の端末装置へ、暗号通信代行承諾データを、前記第１のネットワークを経由して送り、前記暗号通信代行承諾データを受信した前記第１の端末装置は、非暗号化データを、前記第１のネットワークを経由して、前記暗号通信代行サーバへ送り、前記非暗号化データを受信した暗号通信代行サーバは、前記第２の端末装置へ、前記非暗号化データを暗号化したデータを、前記第１のネットワークと前記ゲートウェイと前記第２のネットワークとを経由して送信する。

【００１８】本発明の第１の暗号通信装置では、アクセスが制限された閉鎖型ネットワークに接続され、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して行わせる。

【００１９】本発明の第２の暗号通信装置では、前記開放型ネットワークに接続された端末装置から、前記開放型ネットワークとゲートウェイと閉鎖型ネットワークとを経由して暗号通信要求データを受信し、前記端末装置に暗号通信承諾データと前記閉鎖型ネットワークに接続された暗号通信代行サーバの指定とを、前記閉鎖型ネットワークとゲートウェイと開放型ネットワークとを経由して送信する。

【００２０】本発明の第３の暗号通信装置では、前記開放型ネットワークに接続された端末装置から、前記開放型ネットワークとゲートウェイと閉鎖型ネットワークとを経由して非暗号化データ又は復号化できない暗号化データを受信し、前記端末装置に暗号通信承諾データと前記閉鎖型ネットワークに接続された暗号通信代行サーバの指定とを、前記閉鎖型ネットワークとゲートウェイと開放型ネットワークとを経由して送信する。

【００２１】本発明の第４の暗号通信装置では、前記開放型ネットワークに接続された端末装置に暗号化データを送信するための暗号通信代行要求データを、前記閉鎖型ネットワークに接続された暗号通信代行サーバに、前記閉鎖型ネットワークを経由して送信する。

【００２２】本発明の第５の暗号通信装置では、前記暗号通信代行サーバからの暗号通信代行承諾データを、前記閉鎖型ネットワークを経由して受信し、前記暗号通信代行サーバへ、前記開放型ネットワークに接続された端末装置に暗号化して送信するためのデータを非暗号化の状態で、前記閉鎖型ネットワークを経由して送信する。

【００２３】本発明の第１の暗号通信代行サーバでは、アクセスが制限された閉鎖型ネットワークに接続され、前記閉鎖型ネットワークに接続された第１の端末装置と、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された第２の端末装置との間の暗号通信を、前記第１の端末装置に代行して行う。

【００２４】本発明の第２の暗号通信代行サーバでは、前記開放型ネットワークに接続された第２の端末装置から、前記開放型ネットワークとゲートウェイと閉鎖型ネットワークとを経由して暗号化データを受信し、前記暗号化データを復号し、前記復号化データを前記閉鎖型ネットワークに接続された第１の端末装置へ、前記閉鎖型ネットワークを経由して送信する。

【００２５】本発明の第３の暗号通信代行サーバでは、前記開放型ネットワークに接続された第２の端末装置から、前記開放型ネットワークとゲートウェイと閉鎖型ネットワークとを経由して、暗号通信代行要求データを更に受信し、前記第２の端末装置に、閉鎖型ネットワークとゲートウェイと開放型ネットワークとを経由して暗号通信代行承諾データを送信する。

【００２６】本発明の第４の暗号通信代行サーバでは、前記閉鎖型ネットワークに接続された第１の端末装置から、前記閉鎖型ネットワークを経由して、非暗号化データを受信し、前記非暗号化データを暗号化し、前記暗号化データを、開放型ネットワークに接続された第２の端末装置に、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して送信する。

【００２７】本発明の第５の暗号通信代行サーバでは、前記開放型ネットワークに接続された前記第２の端末装置に、暗号通信要求データを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して更に送信し、前記開放型ネットワークに接続された前記第２の端末装置から、暗号通信承諾データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して受信し、前記閉鎖型ネットワークに接続された第１の端末装置に、暗号通信代行承諾データを、前記閉鎖型ネットワークを経由して送信する。

【００２８】本発明の第６の暗号通信装置では、アクセスが自由な開放型ネットワークに接続され、前記開放型ネットワークとゲートウェイを経由して接続された閉鎖型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行させる。

【００２９】本発明の第７の暗号通信装置では、前記閉鎖型ネットワークに接続された端末装置に、暗号通信要求データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信し、前記閉鎖型ネットワークに接続された端末装置から、暗号通信承諾データと前記閉鎖型ネットワークに接続された暗号通信代行サーバの指定データとを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信し、前記暗号通信代行サーバに、暗号化データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信する。

【００３０】本発明の第８の暗号通信装置では、前記閉鎖型ネットワークに接続された端末装置に、非暗号化データ又は前記端末装置が復号化できない暗号化データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信し、前記閉鎖型ネットワークに接続された端末装置から、暗号通信依頼データと前記閉鎖型ネットワークに接続された暗号通信代行サーバの指定データとを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信し、前記暗号通信代行サーバに、暗号化データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信する。

【００３１】本発明の第９の暗号通信装置では、前記閉鎖型ネットワークに接続された暗号通信代行サーバに、暗号通信代行要求データを、前記開放型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して更に送信し、前記閉鎖型ネットワークに接続された暗号通信代行サーバから、暗号通信代行承諾データを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信する。

【００３２】本発明の第１０の暗号通信装置では、閉鎖型ネットワークに接続された暗号通信代行サーバから、暗号通信要求データを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信し、前記閉鎖型ネットワークに接続された暗号通信代行サーバに、暗号通信承諾データを、前記開放型閉鎖型ネットワークとゲートウェイと前記閉鎖型ネットワークを経由して送信し、前記閉鎖型ネットワークに接続された暗号通信代行サーバから、暗号化データを、前記閉鎖型ネットワークとゲートウェイと前記開放型ネットワークを経由して受信する。

【００３３】本発明の第１の暗号通信方法は、第１のネットワークと、前記第１のネットワークに接続された第１の端末装置と、前記第１のネットワークに接続された暗号通信代行サーバと、前記第１のネットワークとゲートウェイを介して接続された第２のネットワークと、前記第２のネットワークに接続された第２の端末装置と、を使用する暗号通信方法で、前記第１の端末装置と前記第２の端末装置が暗号通信を行う時、前記第１の端末装置に代わって前記暗号通信代行サーバが暗号化と復号化を実行する。

【００３４】本発明の第２の暗号通信方法は、アクセスが制限された閉鎖型ネットワークに接続された暗号通信装置が実行する暗号通信方法で、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して実行させる。

【００３５】本発明の第３の暗号通信方法は、アクセスが制限された閉鎖型ネットワークに接続された暗号通信代行サーバが実行する暗号通信方法で、前記閉鎖型ネットワークに接続された第１の端末装置と、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された第２の端末装置との間の暗号通信を、前記第１の端末装置に代行して実行する。

【００３６】本発明の第４の暗号通信方法は、アクセスが自由な開放型ネットワークに接続された暗号通信装置が実行する暗号通信方法で、前記開放型ネットワークとゲートウェイを経由して接続された閉鎖型ネットワーク

に接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して実行させる。

【００３７】本発明の第１の暗号通信プログラムは、第１のネットワークと、前記第１のネットワークに接続された第１の端末装置と、前記第１のネットワークに接続された暗号通信代行サーバと、前記第１のネットワークとゲートウェイを介して接続された第２のネットワークと、前記第２のネットワークに接続された第２の端末装置と、で実行されるコンピュータプログラムで、前記第１の端末装置と前記第２の端末装置が暗号通信を行う時、前記第１の端末装置に代わって前記暗号通信代行サーバが暗号化と復号化を実行する。

【００３８】本発明の第２の暗号通信プログラムは、アクセスが制限された閉鎖型ネットワークに接続された暗号通信装置で実行されるコンピュータプログラムで、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して実行させる。

【００３９】本発明の第３の暗号通信プログラムは、アクセスが制限された閉鎖型ネットワークに接続された暗号通信代行サーバで実行されるコンピュータプログラムで、前記閉鎖型ネットワークに接続された第１の端末装置と、前記閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された第２の端末装置との間の暗号通信を、前記第１の端末装置に代行して実行する。

【００４０】本発明の第４の暗号通信プログラムは、アクセスが自由な開放型ネットワークに接続された暗号通信装置で実行されるコンピュータプログラムで、前記開放型ネットワークとゲートウェイを経由して接続された閉鎖型ネットワークに接続された端末装置との暗号通信を、前記閉鎖型ネットワークに接続された暗号通信代行サーバに代行して実行させる。

【００４１】本発明の暗号通信プログラムを記録した記録媒体は、上記の何れかのコンピュータプログラムを記録する。

【００４２】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して詳細に説明する。

【００４３】（実施の形態１）図１は本発明の実施の形態１の暗号通信装置を使った暗号通信システムの構成を示すブロック図である。図１のホームネットワーク１０４は第１のネットワークの一実施の形態であり、アクセスが制限された閉鎖型ネットワークの一実施の形態である。家庭内ノード（電子レンジ）１２２、家庭内ノード（エアコン）１２４、家庭内ノード（冷蔵庫）１２６、家庭内ノード（テレビ）１２８の何れかは、前記閉鎖型ネットワークに接続された第１の端末装置の一実施の形態である。

【００４４】尚、この実施の形態では、閉鎖型ネットワークに接続された実施の形態１として、上記のものとしたが、これらは上記のものに限られることは無く、ビデオレコーダー、ビデオカメラ、オーディオ機器、ラジオ、冷蔵庫、電子レンジ、オーブン、トースター、洗濯機、乾燥機、掃除機、エアコン、照明器具、その他家庭内に存在するあらゆる電気製品が可能であり、更に、携帯情報端末、携帯電話、カーナビ、セットトップボックス等の電気製品も可能であり、その他、例えば、パーソナルコンピュータ、電話、ファクシミリ、複写機、オフィースコンピュータ等の企業で使われる事務用電子機器も可能であり、その他あらゆる電気製品が可能である。

【００４５】又、本実施の形態では閉鎖型ネットワークは家庭内に設置されたホームネットワークであるが、必ずしもホームネットワークに限定されるものでは無く、企業内ネットワーク、学校内ネットワーク、地域ネットワーク、その他アクセスが特定のユーザや端末装置に制限されるネットワークならば何であっても良い。或いは、必ずしもアクセスが特定のユーザ等に限定されないネットワークでも可能である。

【００４６】図１の家庭内サーバ（暗号代行）１２０は、本発明の暗号通信代行サーバの一実施の形態である。これは家庭内に設置された情報処理装置であるが、前記家庭内ノードの一つ或いは複数が兼ねることも可能であり、一つの独立した電気製品である家庭内ノードであっても良い。

【００４７】図１のＷＡＮ（インターネット）１０２は、第２のネットワークの一実施の形態であり、アクセスが自由な開放型ネットワークの一実施の形態である。

【００４８】ホームゲートウェイ１０８は、これら閉鎖型ネットワークと開放型ネットワークの各実施の形態である、ホームネットワーク１０４とインターネット１０２を接続するゲートウェイの一実施の形態である。

【００４９】尚、本実施の形態では開放型ネットワークはＷＡＮの一例であり、インターネットであるが、必ずしもインターネットに限定されるものでは無く、ＣＡＴＶネットワークや企業ネットワーク、或る通信キャリアが提供するネットワーク等、アクセスが完全に自由では無く、或る程度の制限を受けるものであっても良い。即ち、前記閉鎖型ネットワークと比較して、閉鎖型ネットワークよりも多くのユーザ、端末装置がアクセス可能なネットワークならば何であっても良い。或いは、必ずしもアクセスが自由なネットワークに限られるものでは無く、アクセスに対する制限が存在するネットワークでも良い。

【００５０】図１の外部ノード１０６は、上記開放型ネットワークに接続された第２の端末装置の実施の形態であり、パーソナルコンピュータ、モバイルパソコン、携帯情報端末、携帯電話、カーナビ、セットトップボック

ス等、その他固定電話、ファクシミリ、複写機、オフィースコンピュータ等の企業で使われる事務用電子機器等、その他家庭で使われる電気機器、その他あらゆる電気製品が可能である。

【００５１】本実施の形態では、図１に示す各家庭内ノードと外部ノード間で暗号通信を行う。各家庭内ノード（１２２～１２８）は、暗号化と復号化の処理を行うために充分なデータ処理性能を有していないため、外部ノード１０６と暗号化通信を行うためのデータ暗号化と復号化の処理を、家庭内サーバ１２０に代行させる。家庭内サーバ１２０は、外部ノード１０６と家庭内ノード間の暗号通信のための暗号化と復号化の処理を、これらの家庭内ノード（１２２～１２８）に代わって行う。

【００５２】外部ノード１０６が暗号通信の起動を行う時の本実施の形態の作用を図１、図２を使って説明する。暗号通信の起動を行う外部ノード１０６は、インターネット１０２、ホームゲートウェイ１０８、ホームネットワーク１０４を経由して暗号通信要求バケットを、暗号通信を行う相手、例えば一つの家庭内ノードである電子レンジ１２２に送る（Ｓ２１）。

【００５３】このデータは、例えば、外部ノード１０６が家庭内ノードである電子レンジ１２２と暗号通信を確立するために必要なデータであり、具体的には、「その電子レンジが暗号通信に対応しているのか否か、或いは対応しているならばその暗号アルゴリズムは何か、更にその暗号鍵は公開されているのか秘匿されているのか、その鍵を入手する方法は何か」等を電子レンジに問い合わせるデータであり、或いは例えば、「暗号鍵が公開されているのならばそれを送れ」とか、「暗号通信に対応していないのならば、他の何らかの方法で暗号通信を行う方法はあるのか、例えば暗号通信代行サーバは存在するのか、もしもそれが存在するのならばそれを知らせよ」等を電子レンジに対して指示するデータであり、或いはその他のデータである。

【００５４】本発明の一実施の形態の家庭内ノードである電子レンジ１２２は、このような暗号通信要求バケットを受信したならば、外部ノード１０６に対して、逆の経路で暗号通信承諾バケットを送信する（Ｓ２２）と同時に、自分に代わって暗号通信の代行を行うサーバを指定する（Ｓ２２）。

【００５５】本実施の形態では、この暗号通信の代行を行うサーバは、同じホームネットワーク１０４に接続された家庭内サーバ１２０であり、外部ノード１０６に送信するデータには、この家庭内サーバのネットワークアドレスが含まれる。

【００５６】又、本発明の一実施の形態の家庭内ノードである電子レンジ１２２は、上記のような暗号通信要求バケットだけでなく、非暗号化データバケットや、自分自身が復号化できない暗号化データバケットを受信した時にも、外部ノード１０６に対して、逆の経路で暗号通信依頼バケットを送信する（図４のＳ４２）と同時に、自分に代わって暗号通信の代行を行うサーバを指定する（図４のＳ４２）。

【００５７】外部ノードから受信した暗号化されていないデータバケットは、セキュリティが全く保障されておらず、そのデータを信頼して受信し、何らかの動作をしたり、応答を行うことは危険であるためである。例えば、電子レンジが受信した非暗号化データが「当日の何時何分になったら電子レンジの加熱モードを１時間ＯＮせよ」等の電子レンジに対する動作指示データであったとする。

【００５８】このようなデータを信頼して受信し、その指示に従うと、いたずらで何の係わりも無い他人に、何の理由も無く電子レンジを１時間以上ＯＮされてしまうこともあり、火事の原因ともなり得るからである。

【００５９】従って、このような非暗号化データを受信した、家庭内ノードである電子レンジはそのデータを無視し、即ちそのデータに従って何らかの動作や応答は行わず、それに代えて、送信元である外部ノード１０６に対して、逆の経路で暗号通信依頼バケットを送信する（図４のＳ４２）と同時に、自分に代わって暗号通信の代行を行うサーバを指定する（図４のＳ４２）。或いは、家庭内ノードである電子レンジ１２２が、自分自身が復号化できない暗号化データバケットを受信した時も同様である。

【００６０】家庭内ノードである電子レンジ１２２が復号化できないデータであるならば、元々、そのデータを解読したり、そのデータの内容に従ったり、そのデータに応答することはできない。

【００６１】従って、そのデータの送信元である外部ノード１０６に対して、逆の経路で暗号通信依頼バケットを送信する（図４のＳ４２）と同時に、自分に代わって暗号通信の代行を行うサーバを指定する（図４のＳ４２）。元来、家庭内ノードである電子レンジ１２２は、高度な処理能力を持っていないので、暗号化データを受信した時、このように、外部ノード１０６に対して、逆の経路で暗号通信依頼バケットを送信する（図４のＳ４２）と同時に、自分に代わって暗号通信の代行を行うサーバを指定する（図４のＳ４２）こととなるケースが多い。

【００６２】しかし、必ずしもこれに限ることは無く、家庭内ノードである電子レンジ１２２も、或る程度の暗号処理機能を有していることもある。この暗号は前記暗号よりも通常は低レベルのものである。このような時は、家庭内ノードである電子レンジが復号化可能な暗号化データを受信することもあり、このケースでは、必ずしも、外部ノード１０６に対して、逆の経路で暗号通信依頼バケットを送信するとは限らない。

【００６３】家庭内ノードである電子レンジが、送信元である外部ノード１０６に対して、逆の経路で暗号通信

依頼パケットを送信する（図４のＳ４２）と同時に、自分に代わって暗号通信の代行を行うサーバを指定した時（図４のＳ４２）の、これ以降の手順を、図４に示す。しかしこの手順は、基本的に外部ノード１０６から、暗号通信要求パケットを受信した時（図２のＳ２１）と同様であるから、以降の説明は、図２を使った、暗号通信要求パケットを受信した時の説明で代用する。

【００６４】暗号通信を行う相手に対して、暗号通信要求パケットを送り（図２のＳ２１）、その相手から暗号通信承諾パケットと同時に、暗号通信代行サーバの指定を受信した（図２のＳ２２）外部ノード１０６は、指定された暗号通信代行サーバである家庭内サーバ１０４に対して、インターネット１０２、ホームゲートウェイ１０８、ホームネットワーク１０４を経由して、暗号通信代行要求パケットを送信する（Ｓ２３）。

【００６５】暗号通信代行要求パケットを受信した家庭内サーバ１２０は、暗号通信代行承諾パケットを、その外部ノード１０６に送信する（Ｓ２４）。これによって外部ノード１０６は、家庭内サーバ１２０が、家庭内ノード１２２（電子レンジ）との暗号通信を代行することを確認する。

【００６６】尚、他の実施の形態では、これらの暗号通信の要求と承諾、暗号通信代行の要求と承諾の手順の全部又は一部を省略することも可能であり、各手順を実行する順序を上記以外の順序と違う順序で行うことも可能である。

【００６７】外部ノード１０６は、家庭内サーバ１２０が、家庭内ノード１２２との暗号通信を代行して行うことを確認した後、或いは、これらの確認の全部又は一部を省略して、予め定められた所定の手順に従って暗号化されたデータパケットを家庭内サーバ１２０に送信する（Ｓ２５）。

【００６８】この暗号化の所定の手順は、一般的な共通鍵暗号方式或いは公開鍵暗号方式、その他の暗号方式を使用することができる。

【００６９】予め定められた所定の手順に従って暗号化されたデータパケットを受信した家庭内サーバ１２０は、その手順に従って暗号化されたデータパケットを復号化し、ホームネットワーク１０４を経由して、本来の通信相手であるべき家庭内ノード１２２（電子レンジ）にその復号化されたデータパケットを送信する（Ｓ２６）。これによって、家庭内ノード１２２（電子レンジ）は、高度な暗号化、復号化のための処理能力を有していなくても、本来の目的である外部ノード１０６との暗号通信を実現することができる。

【００７０】本実施の形態では、ホームネットワーク１０４は、ホームゲートウェイ１０８を介して、外部のネットワークであるインターネット１０２と切り離され、アクセスが制限された閉鎖的ネットワークであるので、復号化されたデータ（暗号化されていないデータ）がこのホームネットワークを経由して通信されてもセキュリティを一層確保することができる。

【００７１】アクセスが自由な開放型ネットワークであるインターネットを経由した通信は、外部ノード１０６と家庭内サーバ１２０の間で、暗号化して行われるため、セキュリティは一層確保される。

【００７２】（実施の形態２）本発明の実施の形態２として、家庭内ノード１２２（電子レンジ）が暗号通信の起動を行う時の本発明の実施の形態の作用を図１、図３を使って説明する。本実施の形態の説明では、上記実施の形態で説明したのと同じ名称、同じ記号を付したものは同一のものを示すので、説明を省略する。

【００７３】暗号通信の起動を行う家庭内ノード１２２（電子レンジ）は、第１のネットワークの一実施の形態であり、閉鎖型ネットワークの一実施の形態である、ホームネットワーク１０４を経由して、暗号通信代行サーバの一実施の形態である家庭内サーバ１２０に、暗号通信代行要求パケットを送信する（Ｓ３１）。

【００７４】この暗号通信代行要求パケットは、暗号通信の代行を要求する旨のデータと同時に、暗号通信を行う相手、本実施の形態では例えば、第２のネットワークの一実施の形態であり、開放型ネットワークの一実施の形態であるインターネットに接続された外部ノード１０６の指定、即ちそのネットワークアドレスを含んでいる。

【００７５】暗号通信代行要求パケットを受信した家庭内サーバ１２０は、暗号通信の代行を要求された相手である外部ノードに対してそのネットワークアドレスに従って、ホームネットワーク１０４、ホームゲートウェイ１０８、インターネット１０２を経由して、暗号通信要求パケットを送信する（Ｓ３２）。

【００７６】暗号通信要求パケットを受信した外部ノードは、暗号通信を了承するならば、家庭内サーバ１２０に対して、逆の経路で、暗号通信承諾パケットを送信する（Ｓ３３）。

【００７７】暗号通信承諾パケットを受信した家庭内サーバ１２０は、暗号通信代行承諾パケットを、暗号通信の要求元である家庭内ノード１２２（電子レンジ）に対して、ホームネットワークを経由して、送信する（Ｓ３４）。

【００７８】尚、本実施の形態では、暗号通信代行要求パケットを受信した（Ｓ３１）、家庭内サーバ１２０は、暗号通信を行う相手である外部ノード１０６に対して、暗号通信要求パケットを送信し（Ｓ３２）、相手の外部ノード１０６から、暗号通信承諾パケットを受信し（Ｓ３３）、暗号通信の要求元である家庭内ノード１２２（電子レンジ）に対して、暗号通信代行承諾パケットを送信した（Ｓ３４）が、他の実施の形態では、これらの暗号通信確認手順（Ｓ３１～Ｓ３４）の全部又は一部を省略することも可能であり、又、これらの確認手順を

実行する順序の全部又は一部を入れ替えて行うことも可能である。

【００７９】更に、これらの確認手順の全部又は一部を暗号化したデータで行うことも可能であり、暗号化しないデータで行うことも可能であり、暗号化して行う場合には、本来のデータの暗号化方式と同一暗号化方式を採用することも可能であり、異なる暗号化方式を採用することも可能である。

【００８０】以上の暗号通信代行要求手順とその暗号通信確認手順の後、又は、これらの手順の全部又は一部を省略して、暗号通信の要求元である、家庭内ノード１２２（電子レンジ）は、非暗号化データパケットを暗号通信代行サーバの一実施の形態である家庭内サーバ１２０に送信する（Ｓ３５）。

【００８１】この非暗号化データパケットを受信した家庭内サーバ１２０は、予め定められた暗号化手順に従って、非暗号化データを暗号化し、暗号化パケットとして、指定された通信相手である外部ノード１０６に送信する（Ｓ３６）。

【００８２】本発明の第１のネットワークが例えば本実施の形態のように、アクセスが制限された閉鎖型ネットワークである場合に、セキュリティが一層確保されることは、前の実施の形態と同様であるから説明を省略する。

【００８３】（実施の形態３）本発明の実施の形態３として、上記実施の形態１で説明した機能と、上記実施の形態２で説明した機能を併せ持つ、暗号通信装置、暗号通信システムの実施の形態があるが、この実施の形態の詳細は、上記実施の形態１と実施の形態２の両方を併せ持つものとして、繰り返すこととなるので説明を省略する。

＊【００８４】尚、本発明に係る発明は、コンピュータとプログラムで実施されることがあり、そのプログラムは記録媒体に記録されることがある。

【００８５】

【発明の効果】本発明によると、いわゆる家庭内電気製品等の高度な情報処理能力を有さない、機器であっても、外部の開放型ネットワークを経由し、高度な暗号通信を行うことが可能であり、そのセキュリティを高度に確保することが出来、その実用的価値は大きい。

【図面の簡単な説明】

【図１】本発明の暗号通信システムの一実施の形態の構成図

【図２】本発明の暗号通信システムの一実施の形態の主構成と通信手順を示す図

【図３】本発明の暗号通信システムの他実施の形態の主構成と通信手順を示す図

【図４】本発明の暗号通信システムの一実施の形態の主構成と通信手順を示す図

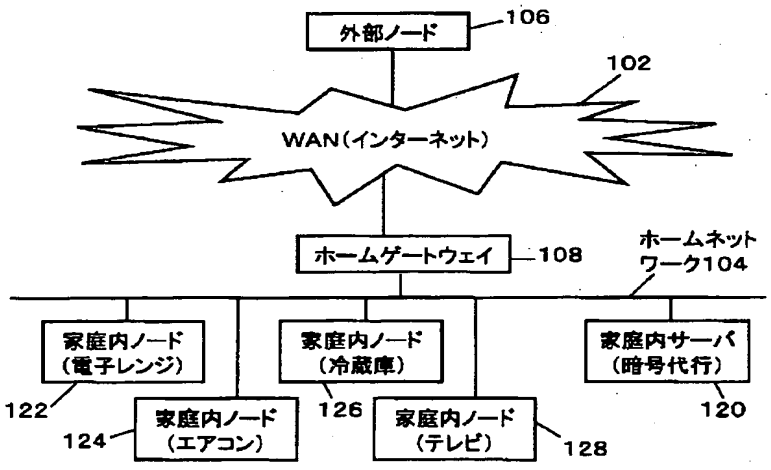
【図５】従来の暗号代行システムの構成と通信手順を示す図

【符号の説明】

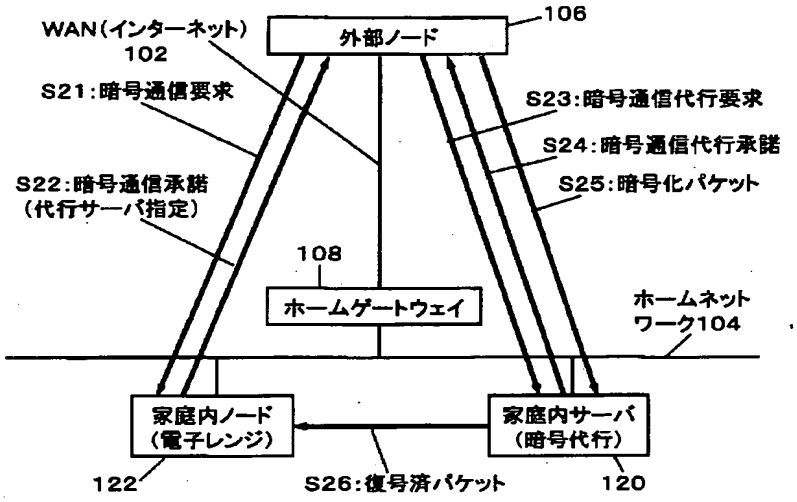
１０２　ＷＡＮ（インターネット）
１０４　ホームネットワーク
１０６　外部ノード
１０８　ホームゲートウェイ
１２０　家庭内サーバ（暗号代行）
１２２　家庭内ノード（電子レンジ）
１２４　家庭内ノード（エアコン）
１２６　家庭内ノード（冷蔵庫）
１２８　家庭内ノード（テレビ）

＊

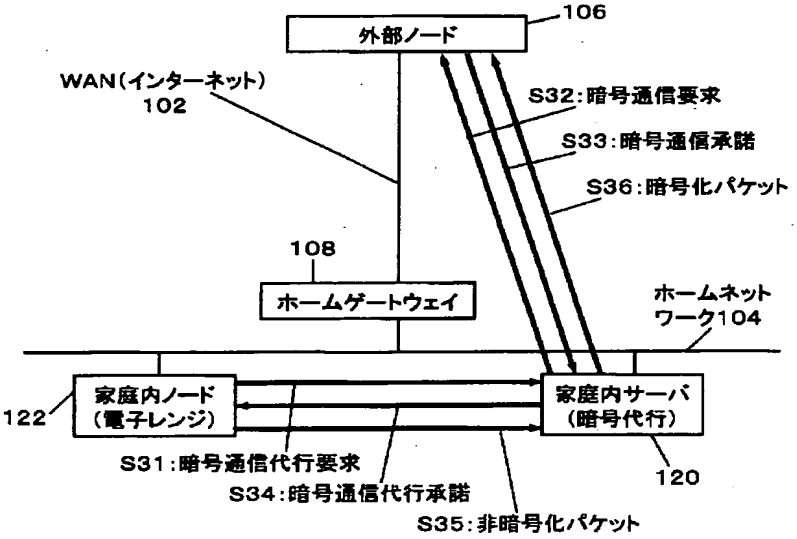
【図１】



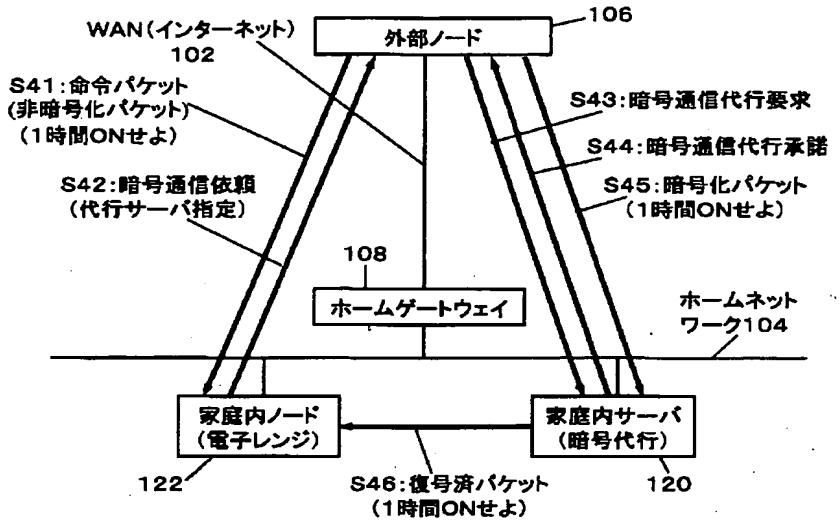
【図２】


WAN(インターネット)
102
外部ノード
106
S21:暗号通信要求
S23:暗号通信代行要求
S24:暗号通信代行承諾
S22:暗号通信承諾
(代行サーバ指定)
S25:暗号化パケット
108
ホームゲートウェイ
ホームネット
ワーク104
家庭内ノード
(電子レンジ)
家庭内サーバ
(暗号代行)
122
S26:復号済パケット
120

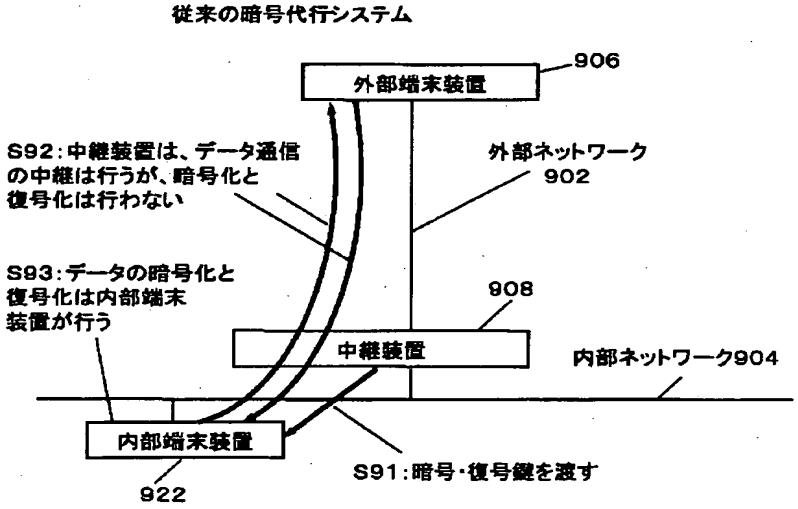
【図３】


外部ノード
106
WAN(インターネット)
102
S32:暗号通信要求
S33:暗号通信承諾
S36:暗号化パケット
108
ホームゲートウェイ
ホームネット
ワーク104
家庭内ノード
(電子レンジ)
122
家庭内サーバ
(暗号代行)
S31:暗号通信代行要求
S34:暗号通信代行承諾
S35:非暗号化パケット
120

【図４】


WAN(インターネット)
102
外部ノード
106
S41:命令パケット
(非暗号化パケット)
(1時間ONせよ)
S43:暗号通信代行要求
S44:暗号通信代行承諾
S42:暗号通信依頼
(代行サーバ指定)
S45:暗号化パケット
(1時間ONせよ)
108
ホームゲートウェイ
ホームネット
ワーク104
家庭内ノード
(電子レンジ)
家庭内サーバ
(暗号代行)
122
S46:復号済パケット
(1時間ONせよ)
120

【図５】


従来の暗号代行システム
外部端末装置
906
S92:中継装置は、データ通信
の中継は行うが、暗号化と
復号化は行わない
外部ネットワーク
902
S93:データの暗号化と
復号化は内部端末
装置が行う
908
中継装置
内部ネットワーク904
内部端末装置
S91:暗号・復号鍵を渡す
922